

Re: new factoring algorithm

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-05/2312.html>

From: Bill Unruh (unruh_at_string.physics.ubc.ca)

Date: 05/30/03

Date: 30 May 2003 00:00:59 GMT

kooshiar62@yahoo.com (kooshiar azimian) writes:

]We present a new algorithm for factoring extending the idea of
]Quadratic Sieve Factoring we can show that it works faster than
]Quadratic Sieve asymptotically .how can we check our algorithm to see
]its new or not ?

assymptotically the Number field sieve is faster already than the
Quadratic sieve. ($\exp(L^{1/3} \ln L^{2/3})$ rather than $\exp(L^{1/2} \ln L^{1/2})$ where L is
the length of the number if I remeber correctly)